AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

DROPBOX ACCOUNTS ASSOCIATED WITH THE EMAIL ACCOUNT D3MHA@LIVE.COM STORED AT A PREMISES CONTROLLED BY DROPBOX

Case No. 18-811M(NJ)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: 18 U.S.C. §§ 1028, 1028A, 1030, and 1343

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

IRS-CI Special Agent Daniel Schmeichel
Printed Name and Title

Sworn to before me and signed in my presence:

Date: March 13, 2018

Judge's signature

City and State: Milwaukee, Wisconsin

Nancy Joseph, U.S. Magistrate Judge
Printed Name and Title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Daniel S. Schmeichel, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Dropbox to disclose to the government copies of the information, including the content of communications associated with email address d3mha@live.com. The account is further described in Attachment A. The information to be disclosed by Dropbox is described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with Internal Revenue Service, Criminal Investigation ("IRS-CI") and have been since February 2010. As an IRS-CI Special Agent, my duties include the investigation of criminal violations of Title 26 (the Internal Revenue Code), Title 31 (the Bank Secrecy Act), and Title 18 of the United States Code. I am currently a member of the Federal Bureau of Investigation Cybercrime Task Force, where I work with FBI agents and task force officers of the FBI on cases involving unauthorized computer intrusions and the theft of personal identifying information, among other federal offenses. Prior to my employment with IRS-CI, I worked a total of approximately five years as a business systems analyst, network manager, and as a computer and network specialist.

3. The statements in this affidavit are based on my personal knowledge, information I have received from other law enforcement personnel, publically available information, and from persons with knowledge of relevant facts. Because this affidavit is being submitted for the limited

purpose of securing a search warrant, I have not included every fact known to me concerning this investigation.

4. Based on the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that the information associated with the accounts identified in Attachment A containing fruits, evidence, and instrumentalities related to violations of Title 18, United States Code, Sections 1030(a)(2)(C) and (a)(5)(A), 1343, 1028, and 1028A (the "Subject Offenses"), as described in Attachment B.

BACKGROUND OF THE INVESTIGATION

5. Since March 2017, the FBI and IRS-CI have been investigating an individual using the online alias "AnonyT." As described in more detail below, AnonyT sold stolen personal identifying information, including names and social security numbers ("PII") through an internet marketplace. During the course of the government's investigation of AnonyT, the FBI and IRS-CI identified several accounts used to facilitate the commission of the Subject Offenses. As described below, probable cause exists to believe the Dropbox account associated with the email address identified in Attachment A was used to facilitate the commission of the Subject Offenses.

6. Based on my training and experience, information from other experienced agents, and the information described below, I believe information, including the contents of communications associated with the account identified in Attachment A will contain fruits, evidence, and instrumentalities related to the Subject Offenses, namely the identity, location, and scope of the criminal activity of individuals associated with the alias "AnonyT."

FACTS IN SUPPORT OF PROBABLE CAUSE[1]

7. On or about March 1, 2017, agents from IRS-CI learned of an advertisement on AlphaBay[2], an illicit internet marketplace, offering to sell tax-related data obtained from Company A.[3] An unidentified individual, using the online moniker "AnonyT," was listed as the contact on the advertisement.

8. On or about March 2, 2017, AnonyT had an instant messaging conversation with an individual, who unbeknownst to AnonyT was a confidential source of information working for the FBI ("CS-1")[4]. During the instant messaging conversation, AnonyT agreed to sell the tax-related data to CS-1 in exchange for $2,000 in bitcoin. A short time later, as directed by AnonyT, a FBI agent transferred 1.68542152 bitcoin (valued at the time at approximately $2,000) to the bitcoin address 14KeaGNUV86CwGv27GWpncuS6gsLKgCgZP. After the bitcoin transfer, AnonyT sent a username and password for a Dropbox[5] account to CS-1. The Dropbox username was email address sta.lampert@gmail.com. An agent successfully used the username and

---

1 At various points in this affidavit, I will offer my interpretation of certain conversations and the meaning to certain terms in brackets. My interpretation of these conversations is based on my knowledge of the investigation to date, conversations with other law enforcement officers and agents, and my experience and familiarity with these types of investigations. The summaries of conversations do not include all potentially criminal conversations during this investigation, or all statements or topics covered during the course of the conversation. The quoted conversations in this affidavit do not represent finalized transcripts and may not represent the entire conversation that occurred between the identified individuals.

2 According to information that was publically available on AlphaBay, AnonyT became active on AlphaBay on or about September 8, 2015. According to information obtained from a private cyber security firm, between September 15, 2015 and May 2017, AnonyT was responsible for approximately 674 posts on AlphaBay that mostly related to the sale of PII.

3 The advertisement also offered remote desktop access to Company A's computer network. Remote desktop access was likely a reference unauthorized access to Company A's computer network through an attack vector that utilized Remote Desktop Protocol.

4 CS-1 has been cooperating with U.S. law enforcement since 2014. CS-1 has no prior criminal convictions. CS-1 is cooperating with the hope of avoiding prosecution for computer related offense or a reduced charge. CS-1 has provided law enforcement with timely and reliable information that has been corroborated through subsequent recorded conversation and controlled buys.

5 As described in more detail below, Dropbox is a remote computing service that offers a file-sharing platform.

password obtained from AnonyT to access the Dropbox account and download approximately 55 GB of tax-related data that contained PII.

9. On March 3, 2017, agents confirmed with the owners of Company A that the data contained in the Dropbox account had been exfiltrated from Company A without authorization. The data included completed IRS tax forms 1040, W-2, and 1099 for Company A's clients.

10. On or about May 5, 2017, the U.S. Magistrate Judge William E. Duffin issued an order pursuant to 18 U.S.C. § 2703(d) requiring Google to disclose to the United States subscriber information for all accounts linked by internet browser cookie to Gmail account sta.lampert@gmail.com.

11. On May 30, 2017, Google provided records for approximately 150 email accounts that "accessed a machine using the same authentication cookie(s) as sta.lampert@gmail.com . . . ." Based on my training and experience, and information obtained from other experienced agents, I understand this to mean that all the email accounts identified by Google were accessed using the same computer. Identified in those records were email accounts: hmooood89@gmail.com and abd.alshanti@gmail.com.

12. According to the records obtained from Google, hmooood89@gmail.com is subscribed to the name Ahmed Alshanti and it was created on July 7, 2006.

13. According to Google records, abd.alshanti@gmail.com is subscribed to the name Abd Alshanti. Google records listed info@unknown.ps as the recovery email address[6] for abd.alshanti@gmail.com.

14. According to Google records info@unknown.ps is subscribed to the name Abdulrhman Alshanti. According to Google records, info@unknown.ps is the recovery email

---

6 The recovery email account is used to recover forgotten passwords.

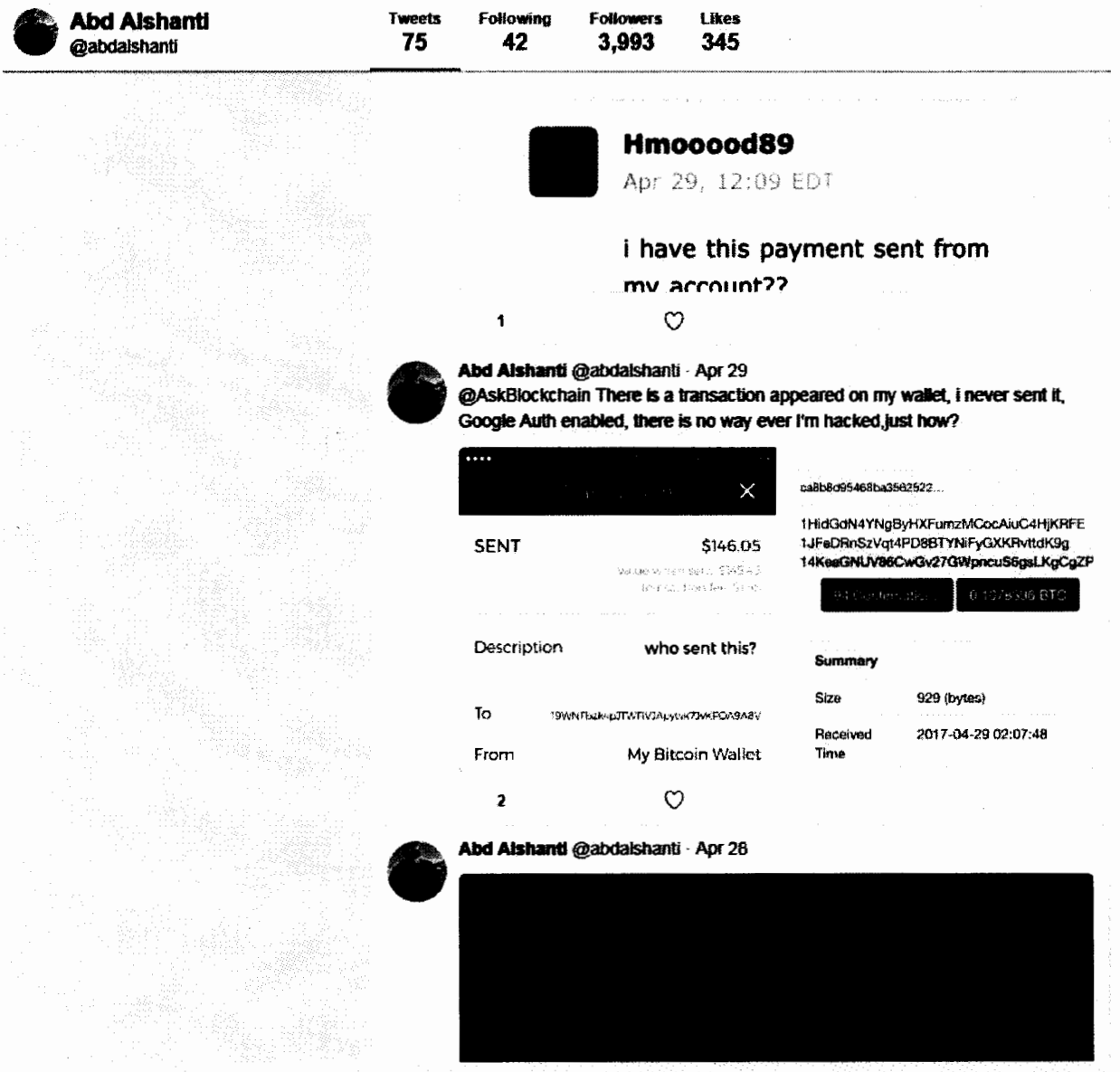
address for and at least three of the other email accounts linked to the sta.lampert@gmail.com by internet browser cookie. According to Google records, info@unknown.ps was created on March 14, 2010.

15. I reviewed the publicly available information on the internet website unknown.ps, which is the domain[7] for info@unknown.ps. Based on my review of the information on that website, it appears to be a website for Abd Alshanti, which is the subscriber name on abd.alshanti@gmail.com. On the website, an individual believed to be Abd Alshanti describes himself as a "Self-Taught Web Developer and SEO Expert based in Palestine, Gaza Strip." The website is linked to publically accessible Facebook and Twitter accounts for Abd Alshanti and a publically available Instagram account in the name "Bu Ziad." The profile photos displayed on those Facebook, Twitter, and Instagram accounts appeared to be of the same person and all accounts identify the user as being located in Gaza, Palestine.

16. I reviewed the publically available tweets associated with Abd Alshanti's Twitter page for username @abdalshanti. On April 29, 2017, the user of that account sent a tweet to an online bitcoin wallet provider claiming an unauthorized bitcoin payment was made from the bitcoin addresses held in his bitcoin wallet. In the tweet, the user of that account posted a screenshot of an email message that appears to be sent from hmooood89@gmail.com to a bitcoin wallet provider complaining of an unauthorized bitcoin transaction. The user of that account also tweeted screenshots of the completed transaction, showing the bitcoin addresses in his bitcoin wallet that funded the complained of transaction. One of those bitcoin addresses,

[7] A domain name is also the name that identifies a website on the internet. For example, "microsoft.com" is the domain name of Microsoft's website. Like an IP address, a domain name consists of a sequence of characters, separated by periods. Domain names are organized hierarchically and they are read from right to left. The right-most component is the "top level domain." This includes the ".com," ".gov," and ".edu" domains, as well as many others. The second part of the domain name is owned by the registrant who first registered the name.

14KeaGNUV86CwGv27GWpncuS6gsLKgCgZP, was the same bitcoin address used by AnonyT in the transaction with the FBI, described in paragraph 8 above[8]. A copy that tweet is shown below:



[8] As described below, a search warrant was executed on the account hmooood89@gmail.com. During my review of the information associated with that account, I located an email sent to hmooood89@gmail.com on March 2, 2017 from Blockchain.info. The email contained a notice to the account holder that that the bitcoin address 14KeaGNUV86CwGv27GWpncuS6gsLKgCgZP, which was held in his bitcoin wallet, received 1.68542152 bitcoin. This notification was for the transaction in which the FBI purchased the stolen data from AnonyT as described in paragraph 8.

17. On or about June 22, 2017, a grand jury subpoena was issued to Twitter for records related to info@unknown.ps and Twitter username @abdalshanti. On or about August 25, 2017, Twitter produced records responsive to the subpoena. According to records obtained from Twitter, username @abdalshanti is registered to info@unknown.ps.

18. On or about September 27, 2017, U.S. Magistrate Judge David E. Jones issued search warrants requiring Google to provide information, including email communications, for the email accounts hmooood89@gmail.com and info@unknown.ps. Google provided the required information for hmooood89@gmail.com on October 2, 2017. Google provided the required information for info@unkown.ps on October 20, 2017.

19. I reviewed the email communications disclosed by Google for email accounts hmooood89@gmail.com and info@unknown.ps. Based on my training and experience and my knowledge of this investigation, I located several communications associated with those accounts that related to violations of the Subject Offenses. Some of those communications were received from or sent to Microsoft email account d3mha@live.com. For example, the following communications involved the user of account d3mha@live.com:

a. On or about May 24, 2013, the user of account info@unknown.ps and the user of account d3mha@live.com exchanged a number of emails that contained credit card numbers and PII. More specifically, the user of account d3mha@live.com sent an email to the user of account info@unknown.ps that contained a credit card number and PII and wrote, "check if it [the credit card number] works." In response, the user of info@unknown.ps asked where d3mha obtained the credit card and PII information. The user of d3mha@live.com sent a reply email that stated, "http://www.mymobilenation.com [the website that d3mha had breached]." The user of account info@unknown.ps sent an email in response that stated, "you fucking genius I

knew you could do it motherfucker get all the CCs [info@unknown.ps was impressed that d3mha had hacked the website and he wanted d3mha to steal all the available credit card information]."

b. On or about August 20, 2013, the user of account info@unknown.ps sent an email with the subject line "Remote Desktop" to the user of account d3mha@live.com. The body of the email listed IP address 113.212.70.231, and what appeared to be the username and password to establish an RDP[9] connection to the IP address. According to information available from Centralops.net,[10] IP address 113.212.70.231 is owned by APNIC-AP located in Australia.

c. On or about November 11, 2015, the user of account info@unknown.ps sent an email with the subject "new 1and1" to the user of account d3mha@live.com. The body of the email listed IP address 74.208.69.227 and what appeared to be the username and password to that IP address. According to information available from Centralops.net, IP address 74.208.69.227 is owned by 1 & 1 Internet Inc. located in Pennsylvania.

d. On or about February 24, 2016, the user of account info@unknown.ps sent an email with the subject "new srv [server]" to the user of account d3mha@live.com. The body of the email listed IP address 198.251.79.203 and hat appeared to be the password to that IP address. According to information available from Centralops.net, IP address 198.251.79.203 is owned by 1 & 1 Internet Inc. located in Pennsylvania.

e. On December 11, 2016, the user of accountinfo@unknown.ps sent an email with the subject "DO THIS ONCE YOU OPEN LAP!!" to the users of accounts d3mha@live.com

---

9 In this case, I believe the IP address 113.212.70.231 represented a compromised server on which RDP access had been established without authority. Unless otherwise noted, I believe the communication described in this affidavit that involved RDP access to an IP address related to a computer that was accessed without authorization.

10 Centralops.net is publicly available website that lists contact and registry information for domain names and IP addresses.

and hmooood89@gmail.com. The body of the email what appeared to be the username and password for a merchant account on Etsy.com.[11] The email stated, "he [the merchant] have a good (sic) ETSY shop receiving (sic) many payments daily... update the bank account on profile to the new one you created and added to paypal [the merchant's bank account information should be replaced with a different account from PayPal]!! A deposit of $1,537.11 is scheduled for Mon, Dec 12, 2016, act fast!! be sure to check email after!! its good money if he never notice for a month [the owner might not notice the bank account information was changed] . . . log to his [the merchant's] email first to avoid him [the merchant] seeing any changes you'll make." A short time later, the user of account d3mha@live.com replied, "did this [D3mha changed the bank account information for the Etsy account]." According to information obtained from Centralops.net, IP address 98.189.245.28 is owned by Cox Communications.

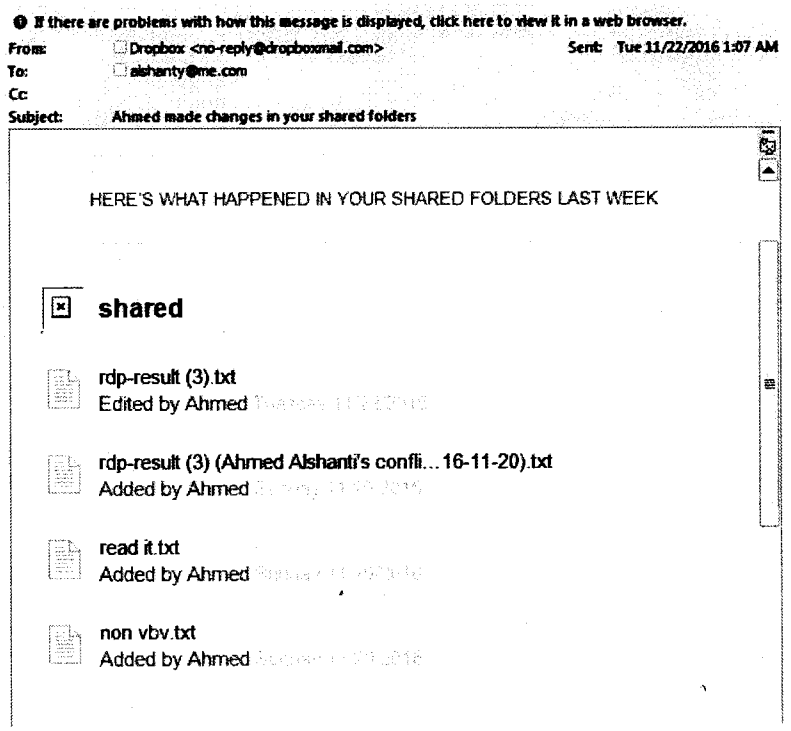
f. On or about July 11, 2017, the user of info@unknown.ps sent an email message to the users of accounts hmooood89@gmail.com and d3mha@live.com. The body of the email stated, "reg [register] now on dream market [a darknet market place for illicit goods and services], every1 [everyone] moving (sic) there [dream market], it may get us [the coconspirators] better sales than hansa [a darknet marketplace for illicit goods and services that was closed by Dutch authorities on July 6, 2017]."

20. I also located emails that identified a Dropbox account the targets of this investigation used to facilitate the commission of the Subject Offenses. For example, on or about February 24, 2015, the user of email account info@unknown.ps received an email from Dropbox. The subject of the email stated, "Ahmed Alshanti wants to share 'work' with you." The body of

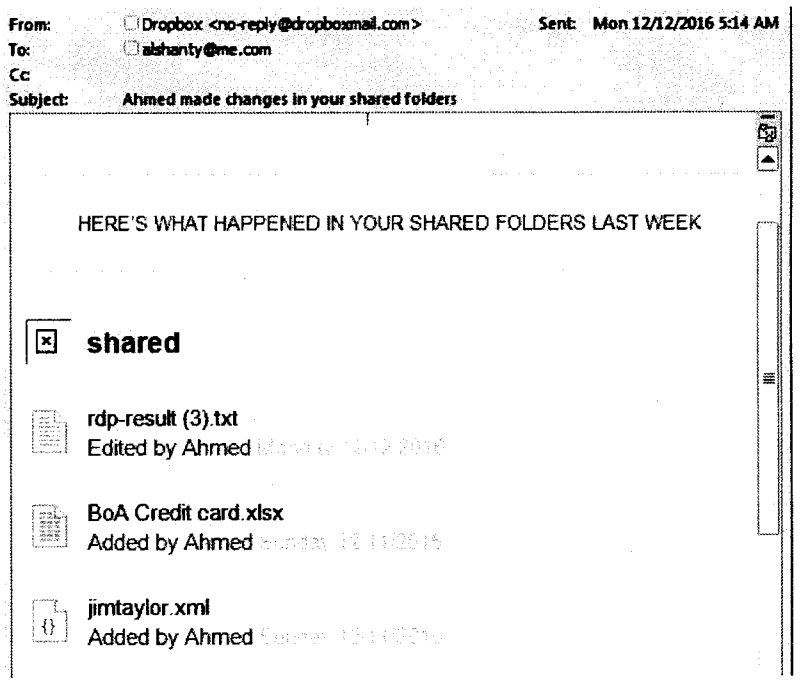
[11] Etsy.com is an online marketplace for various commercial goods and services.

the email stated, "Ahmed (d3mha@live.com) wants to share some files in a folder called 'work' with you via Dropbox."

21. Between on or about November 16, 2016, and September 26, 2017, the user of account info@unknown.ps received approximately 44 email notifications addressed to alshanty@me.com[12] from Dropbox with the subject, "Ahmed made changes in your shared folders." The notification emails from Dropbox to alshanty@me.com stated, "HERE'S WHAT HAPPENED IN YOUR SHARED FOLDERS LAST WEEK." The emails included details about the shared files and folders that had been updated. For example:


If there are problems with how this message is displayed, click here to view it in a web browser.
From: Dropbox <no-reply@dropboxmail.com> Sent: Tue 11/22/2016 1:07 AM
To: alshanty@me.com
Cc:
Subject: Ahmed made changes in your shared folders
HERE'S WHAT HAPPENED IN YOUR SHARED FOLDERS LAST WEEK
shared
rdp-result (3).txt
Edited by Ahmed
rdp-result (3) (Ahmed Alshanti's confli...16-11-20).txt
Added by Ahmed
read it.txt
Added by Ahmed
non vbv.txt
Added by Ahmed

[12] Based on my training and experience, I believe these emails were originally sent to the account alshanty@me.com, and a forwarding feature on that account caused them to be sent the account info@unknown.ps.



From: Dropbox <no-reply@dropboxmail.com> Sent: Mon 12/12/2016 5:14 AM
To: alshanty@me.com
Cc:
Subject: Ahmed made changes in your shared folders

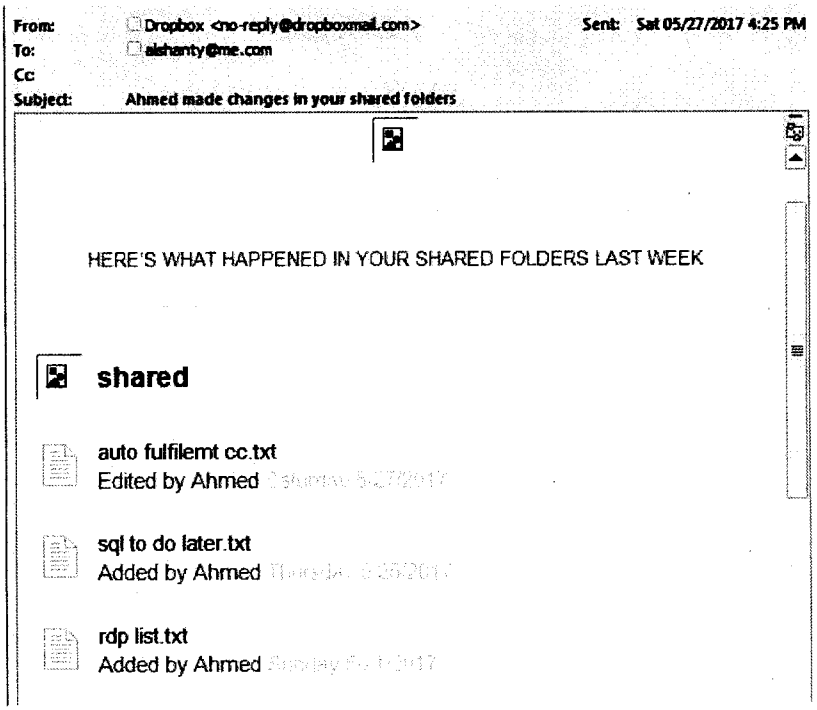
HERE'S WHAT HAPPENED IN YOUR SHARED FOLDERS LAST WEEK

shared

rdp-result (3).txt
Edited by Ahmed

BoA Credit card.xlsx
Added by Ahmed

jimtaylor.xml
Added by Ahmed



From: Dropbox <no-reply@dropboxmail.com> Sent: Sat 05/27/2017 4:25 PM
To: alshanty@me.com
Cc:
Subject: Ahmed made changes in your shared folders

HERE'S WHAT HAPPENED IN YOUR SHARED FOLDERS LAST WEEK

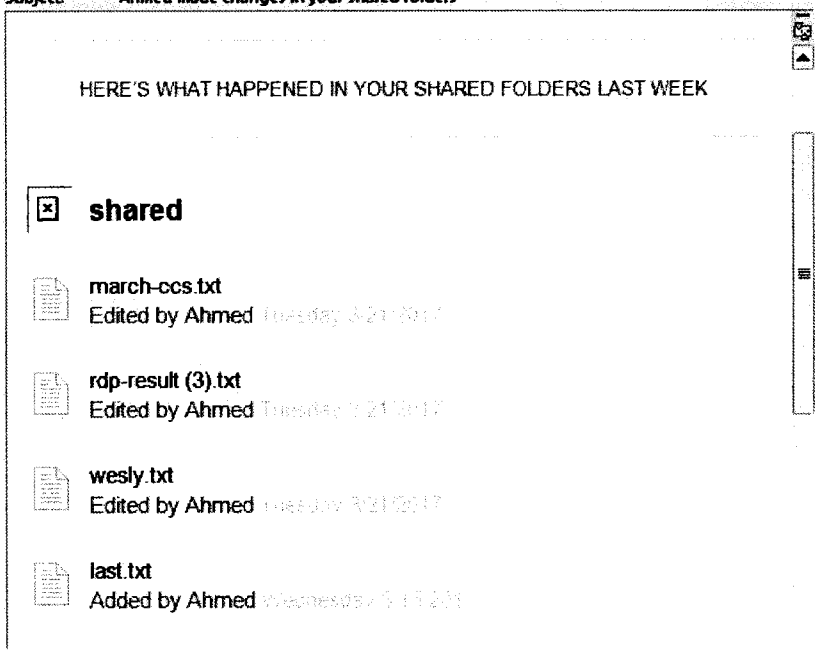
shared

auto fulfilemt cc.txt
Edited by Ahmed

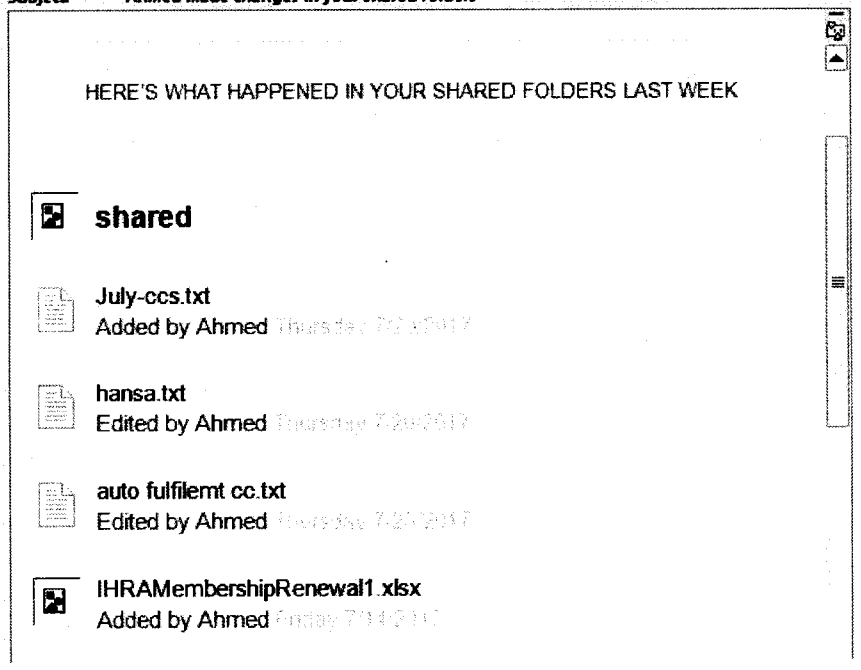
sql to do later.txt
Added by Ahmed

rdp list.txt
Added by Ahmed

From: Dropbox <no-reply@dropboxmail.com> Sent: Tue 03/21/2017 6:57 PM
To: alshanty@me.com
Cc:
Subject: Ahmed made changes in your shared folders



From: Dropbox <no-reply@dropboxmail.com> Sent: Thu 07/20/2017 9:16 AM
To: alshanty@me.com
Cc:
Subject: Ahmed made changes in your shared folders



22. On November 13, 2017, U.S. Magistrate Judge William E. Duffin issued a warrant authorizing the search and seizure of information associated with Dropbox accounts associated with email account alshanty@me.com.

23. On or about December 6, 2017, Dropbox disclosed the responsive materials to me. Based on my knowledge of the investigation, and my review of the information disclosed by Dropbox, I believe the files disclosed by Dropbox contained stolen PII, malware and other information used to compromise computer systems and steal PII, and other information related to the Subject Offenses. Many of these files were contained in a shared folder.

24. On or about January 30, 2018, a representative from Dropbox informed me that Dropbox had additional records and information associated with the shared folder described above and disclosed in response to the warrant issued by Magistrate Judge Duffin, including a complete file activity log showing when the content of the shared folder was added, edited, moved, or renamed.

25. On February 8, 2018, U.S. Magistrate Judge David E. Jones issued a warrant authorizing the search and seizure of information associated with Dropbox accounts associated with email account alshanty@me.com, to include information related to shared folder activity.

26. On or about February 12, 2018, Dropbox disclosed materials in response to the warrant issued by Magistrate Judge Jones. The disclosure included file access and sharing histories of the shared folder and the files contained within it. Based on those records, the shared folder in the alshanty@me.com account, which contained stolen PII, malware and other information used to compromise computer systems and steal PII, and other information related to the Subject Offenses, was originally created by Dropbox user d3mha@live.com. According to Dropbox

records, on or about November 14, 2016, d3mha@live.com shared the folder with alshanty@me.com.

27. The information disclosed by Dropbox also showed which files in the shared folder had been created or edited by alshanty@me.com. Based on this information, it appears that much of the stolen PII, malware and other information used to compromise computer systems and steal PII, and other information related to the Subject Offenses, was originally saved to the shared folder by Dropbox user d3mha@live.com. This includes the file "xRdp.v2.1.exe," which was an executable file detected on one of Company A's computers, and the file "rdp-result (3) (Ahmed Alshanti's conflicted copy 2017-04-10).txt," which contained the text, "216.251.160.225:3389@SM\Administrator;1948 (Tax Files- dropbox acc: sta.lampert@gmail.com/n1)."

28. Based on my experience and knowledge of the investigation to date, I know that the first part of the text file (**216.251.160.225**:3389@SM\Administrator) represents an IP address. I also know that IP address 216.251.160.225 was the public IP address for Company A at the time its computer system was breached. Additionally, as described in paragraph 8, the Gmail account, sta.lampert@gmail.com, was used to obtain and sell PII from Company A.

BACKGROUND CONCERNING DROPBOX

29. Dropbox is a service that allows its users to store files on Dropbox's servers. Dropbox offers both free and fee based services. According to Dropbox's privacy policy, available at https://www.dropbox.com/privacy, Dropbox allows its customers to "collaborate with others" and to store "files, messages, comments, and photos . . . as well as information related to it." To establish an account, Dropbox collects the customer's name, email address, phone number, payment information, and physical address.

30. Dropbox states that it collects information related to how its customers uses its services, "including actions [the customer] take[s] in [the] account (like sharing, editing, viewing, and moving file folders)."

31. Dropbox also collects information "from and about the devices you use to access [Dropbox] services . . . includ[ing] things like IP addresses, the type of browser and device you use, the web page you visited before coming to [the Dropbox] sites, and identifiers associated with [the] devices." Dropbox states that depending on the devices settings, it might also collect location information for the device used to access their services.

32. In some cases, Dropbox users will communicate directly with Dropbox about issues relating to their account, such as technical problems, billing inquiries, or complaints.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

33. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Dropbox to disclose to the government copies of the records and other information (including the content of communications) described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

34. Based on the information described above, I request that the Court issue the proposed search warrant.

35. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) &

(c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

36. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the account(s) related to d3mha@live.com (the "account") that is stored at premises owned, maintained, controlled, or operated by Dropbox Inc., a company headquartered at 333 Brannan Street, San Francisco, California 94107 (the "Provider").

ATTACHMENT B

Particular Things to be Disclosed and Seized

I. Information to be disclosed by Dropbox (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on October 23, 2017, the Provider is required to disclose the following information to the government for the account or identifier listed in Attachment A:

a. All customer information (e.g. name, age, email address, physical address, payment information) associated with the accounts;

b. All records and information regarding the creation account and access to the account, including records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, and log-in IP addresses associated with session times and dates.

c. All records, files, and other information stored/saved in the accounts;

d. All records and information and analytics collected by the Provider through the use of cookies or similar technology including the type of browser and device used by the account holder, the web page visited before coming to Dropbox sites, and other identifiers associated with the devices used by the account holder;

e. All records pertaining to communications between the Provider and any person regarding the accounts, including contacts with support services and records of actions taken;

f. A complete file activity log for shared folders associated with the account; and

g. Information related to the shared folders associated with the account, including Dropbox account information for users accessing those shared folders.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of the warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities related to violations of Title 18, United States Code, Sections 1030(a)(2)(C) and (a)(5)(A), 1343, 1028, and 1028A, since November 2016, including information pertaining to the following matters:

a. The identity of the person(s) who communicated with the user of the account and accessed records and shared folders associated with the account;

b. Information associated with shared folders, including file activity details and log, information identifying the original owner and users of all shared folders, and the details regarding when the shared folders were shared and when users were provided with access to the folders;

c. Information related to the sale and distribution of financial information, credit card numbers, social security numbers, and other personal identifiable information.

d. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s) such as photographs and records related to travel abroad;

e. The identity of the person(s) who communicated with the user of the account including records that help reveal their whereabouts;

f. Files and records that contain financial information, credit card numbers, social security numbers, and other personal identifiable information;

g. Communications and files that contain IP addresses and username and passwords to those IP addresses;

h. Files related to remote desktop protocol and other remote computer access protocols; and

i. Files containing malware.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Dropbox. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of **Dropbox**, and they were made by **Dropbox** as a regular practice; and

b. such records were generated by **Dropbox's** electronic process or system that produces an accurate result, namely:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of **Dropbox** in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by **Dropbox**, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature